This listing of claims will replace all prior versions and listings of claims in this application:

a.) Listing of Claims

1. (currently amended)   In a routing device, a method of operation comprising:

receiving a packet sent by a client device ~~destined for a server~~;

determining if the packet is destined for a server of interest by reference to a destination address of the packet;

if the packet is not destined for the server of interest, routing the packet to its destination;

if the packet is determined to be destined for the server of interest, independently determining whether said packet is a part of a conversation between the client device and the server of interest based at least in part on persistent information included in said packet; and

handling the packet based at least in part on the result of said independent determination by forwarding the packet to the server of interest if the packet is deemed to be a part of a conversation between the client device and the server and dropping the packet if the packet is deemed to be an undesirable packet.

2. (original)   The method of claim 1, wherein said independent determination comprises independently verifying a conversation identifier included in said packet based at least in part on other information included in said packet.

3. (original)   The method of claim 2, wherein said independent verification comprises

independently regenerating the conversation identifier using at least said other information included in said packet; and

comparing the independently re-generated conversation identifier with the included conversation identifier.

4. (original)   The method of claim 3, wherein said conversation identifier is a nonce, and said independent re-generation comprises independently re-generating the nonce

using a deterministic function with a sequence number of the nonce and a plurality of persistent field values extracted from the packet, and a pre-provided secret value as inputs to the deterministic function.

5. (original)   The method of claim 4, wherein said plurality of persistent field values comprise one or more of a source address, a destination address and a port number.

6. (original)   The method of claim 4, wherein the method further comprises at least one of receiving into said routing device said secret value, and equipping/configuring said routing device with said deterministic function.

7. (original)   The method of claim 4, wherein said independent generation is performed using a selected one of a message authentication code function and an universal hash function.

8. (original)   The method of claim 4, wherein the method further comprises recording a time of first observation for the nonce if the nonce is a newly observed nonce.

9. (currently amended)   The method of claim 8, wherein the method further comprises determining if time has elapsed more than a predetermined threshold since a time of first observation was recorded for the nonce, if the extracted nonce and the independently generated nonce are deemed to be the same and dropping the packet if the time has elapsed more than the predetermined threshold event though the extracted nonce and the independently generated nonce are deemed to be the same.

10. (cancelled)

11. (currently amended)   In a server and network, a method of operation comprising:

generating an independently verifiable conversation identifier for a packet destined for a client device, using at least persistent information that will be included in said packet;

including the independently verifiable conversation identifier with said packet for use by the client device to include in a subsequent packet sent by the client device destined for the server; ~~and~~

transmitting said independently verifiable conversation identifier included <u>in the</u> packet to said client device; <u>and</u>

determining whether to forward or drop the packet through a network in response to the conversation identifier to protect the network against undesirable packets <u>by determining if the packet is destined for the server by reference to a destination address of the packet, if the packet is not destined for the server routing the packet to its destination, if the packet is determined to be destined for the server determining whether the packet is a part of a conversation between the client device and the server based at least in part on the persistent information included in said and forwarding the packet to the server if the packet is deemed to be a part of a conversation between the client device and the server and dropping the packet if the packet is deemed to be an undesirable packet</u>.

12. (original) The method of claim 11, wherein said generation of an independently verifiable conversation identifier comprises:

generating a sequence number for a nonce; and

generating the nonce as the independently verifiable conversation identifier for the packet using a deterministic function with the sequence number, a plurality of persistent field values of the packet, and a secret value as input values to the deterministic function.

13. (original) The method of claim 12, wherein said plurality of persistent field values comprise one or more of a source address, a destination address and a port number.

14. (cancelled)

15. (cancelled)

16. (cancelled)

17. (currently amended)   A routing apparatus comprising:

an interface to receive a packet sent by a client device destined for a server; and

a function unit coupled to the interface to independently determine whether said packet is a part of a conversation between the client and the server based at least in part on persistent information included in the packet, and output a packet disposition signal based at least in part on the result of said independent determination

wherein the function unit determines if the packet is destined for the server by reference to a destination address of the packet; if the packet is not destined for the server, routing the packet to its destination; if the packet is determined to be destined for the server, independently determining whether said packet is a part of a conversation between the client device and the server based at least in part on the persistent information included in the packet; wherein the packet disposition signal causes the routing device to forward the packet to the server if the packet is deemed to be a part of conversation between the client device and the server and drop the packet if the packet is deemed to be an undesirable packet.

18. (original) The routing apparatus of claim 17, wherein said function unit is to designed to make said independent determination by independently verifying a conversation identifier included in said packet based at least in part on other information included in said packet.

19. (original) The routing apparatus of claim 18, wherein said function unit comprises

an identifier generator to independently regenerate the conversation identifier using at least said other information included in said packet; and

a comparator coupled to the identifier generator to compare the independently re-generated conversation identifier with the included conversation identifier.

20. (original) The routing apparatus of claim 19, wherein said conversation identifier is a nonce, and said identifier generator is designed to independently re-generate the nonce using a deterministic function with a sequence number of the nonce and a plurality of persistent field values extracted from the packet, and a pre-provided secret value as inputs to the deterministic function.

21. (original) The routing apparatus of claim 20, wherein said identifier generator comprises a deterministic function.

22. (currently amended) A server comprising:

at least one processor; and

a communication interface coupled to the processor to transmit packets to one or more client devices on behalf of the processor including

a generator to generate an independently verifiable conversation identifier for a packet destined for one of said one or more client devices, using at least persistent information that will be included in said packet,

a summing unit to insert the independently verifiable conversation identifier with said packet for use by the particular client device to include in a subsequent packet sent by the client device destined for the server, and

a transmitter to transmit said independently verifiable conversation identifier included packet to said particular client device

wherein a router determines if the packet is destined for the server by reference to a destination address of the packet; if the packet is not destined for the server, routing the packet to its destination; if the packet is determined to be destined for the server, independently determining whether the packet is a part of a conversation between the client device and the server based at least in part on the independently verifiable conversation identifier included in said packet; wherein the routing device to forwardes

the packet to the server if the packet is deemed to be a part of the conversation between the client device and the server and dropping the packet if the packet is deemed to be an undesirable packet..

23. (previously presented) The server of claim 22, wherein said generator comprises

a counter to generate a sequence number for a nonce; and

a deterministic function unit to generate the nonce as the independently verifiable conversation identifier for the packet using the sequence number, a plurality of persistent field values of the packet, and a secret value as input values.

24. (previously presented) The server of claim 23, wherein said plurality of persistent field values comprise one or more of a source address, a destination address and a port number.

25. (previously presented) The server of claim 23, wherein said deterministic function is a selected one of a message authentication code function and a universal hash function.

26. (cancelled)

27. (cancelled)

28. (cancelled)

29. (cancelled)

30. (cancelled)

31. (cancelled)

32. (previously presented) The routing apparatus of claim 17, wherein said function unit drops packets that are not part of the conversation to protect the server against receipt of undesirable packets.